



221 E. Fourth St.
P.O. Box 2301
Cincinnati, Ohio 45201-2301

February 25, 2013

FILED ELECTRONICALLY via ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W., Suite TW-A325
Washington, D.C. 20554

RE: Annual Certification of CPNI Filing (2012)
EB Docket No. 06-36

Dear Secretary Dortch:

Pursuant to the Commission's January 16, 2013 *Public Notice* in the above-referenced proceeding (DA13-61) and section 64.2009(e) of the Commission's rules, Cincinnati Bell Inc., on behalf of its subsidiaries, hereby submits its certificate and accompanying statement demonstrating compliance with the Commission's rules protecting the privacy of customer proprietary network information ("CPNI"), 47 C.F.R. §§ 64.2001-2009, for the year ending December 31, 2012.

If you have any questions or concerns regarding the certification or statement, please do not hesitate to contact me at (513) 397-1375.

Sincerely,

A handwritten signature in cursive script that reads "Ted Heckmann".

Ted Heckmann
Managing Director – Regulatory & Government Affairs

cc: Best Copy and Printing by email to fcc@bcpiweb.com

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012

Date filed: February 25, 2013

Names of companies covered by this certification:

Cincinnati Bell Inc., 499 ID # 825783

Cincinnati Bell Telephone Company LLC, 499 ID # 805713

Cincinnati Bell Extended Territories LLC, 499 ID # 825068

Cincinnati Bell Any Distance Inc., 499 ID # 809872

Cincinnati Bell Wireless LLC, 499 ID # 819126

eVolve Business Solutions LLC, 499 ID #827855

Name of signatory: **John Donbar**

Title of signatory: **Vice President, Internal Audit**

I, John Donbar, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year, and the company does not have information to report with respect to the processes pre-texters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action

Signed: _____

A handwritten signature in black ink, appearing to read "John Donbar", is written over a horizontal line.

Attachment: Statement Regarding CPNI Operating Procedures

CINCINNATI BELL INC.
STATEMENT REGARDING CPNI OPERATING PROCEDURES
February 25, 2013

This statement is filed on behalf of Cincinnati Bell Inc. ("CBI") and the following subsidiaries: Cincinnati Bell Telephone Company LLC ("CBT"), an incumbent local exchange carrier; Cincinnati Bell Any Distance Inc. ("CBAD"), an interexchange carrier; Cincinnati Bell Extended Territories LLC ("CBET"), a competitive local exchange carrier; Cincinnati Bell Wireless LLC ("CBW"), a wireless service provider, and eVolve Business Solutions LLC ("eVolve"), an interconnected VoIP provider.

Employee Training Regarding Protection of CPNI

CBI continually educates and trains its employees on the appropriate use of customers' CPNI. As set forth in CBI's Corporate Policies Manual, it is the policy of CBI to protect the confidentiality of all CPNI in its possession in accordance with Section 222 of the Telecommunications Act of 1996. In addition, CBI's Code of Business Conduct states that employees are required to safeguard any proprietary information received from customers or potential customers as though it were the company's own information. Each year, salaried employees are required to sign a statement acknowledging that the employee has received a copy of the Code of Business Conduct and that the employee has been advised to read the code, become familiar with its contents and abide by the rules and principles set forth in it. Similarly, all hourly employees are provided a copy of the code and are instructed to read and become familiar with its contents. Supervisors of hourly employees are required to sign an attendance roster indicating that the hourly employees participated in awareness training and to submit the roster to the Human Resources Department. The Code of Conduct clearly states that breaches of the principles contained in the policy are grounds for disciplinary action, including dismissal, and may carry penalties under federal and state laws.

Use, Disclosure and Access to CPNI

CBI has adopted specific CPNI policies and procedures to ensure that CPNI is only used, disclosed or accessed to provide or market services among the categories of service to which the customer already subscribes except as permitted by Section 222(d) of the Act and Section 64.2005 of the Commission's rules or where CBI has the customer's approval in accordance with Rule 64.2007. More specifically, CBI has implemented a system by which the status of a customer's CPNI approval can be established prior to the use of CPNI, and CBI's sales consultants are trained to recognize when a customer has or has not approved of the use CPNI for marketing purposes as indicated by the customer's service record. If a customer has not previously approved of the use of CPNI for marketing purposes, either by opt-in or opt-out approval, sales consultants are trained to request the customer's permission to access the customer's records for the duration of the call or in-store visit as necessary.

CBI maintains a record of customers' approval or disapproval to use, disclose or permit access to a customer's CPNI for marketing purposes. A customer's approval or disapproval remains in effect until the customer revokes or limits the approval or disapproval. CBI maintains a record of such CPNI approval or disapproval for a minimum of one year.

Notice Required for Use, Disclosure, or Access to CPNI

CBI policies require that customers be notified of their rights and of the company's legal obligations with respect to CPNI prior to solicitation of customer approval. CBI provides notice to customers containing the disclosures required in Section 64.2008 of the Commission's rules.

Safeguards Required for Use, Disclosure, or Access to CPNI

CBI complies with the Commission's requirement to establish a supervisory review process for outbound marketing processes. Specifically, marketing personnel must submit a request to obtain customer information in order to conduct an outbound campaign. The request must indicate the parameters of the data sought other key information about the campaign, as well as by whom the request is made. The information requested is retrieved by designated personnel and scrubbed to eliminate customers who elect not to share CPNI or who have requested to be placed on the company's do-not-call/contact list. CBI maintains a record of all sales and marketing campaigns that use customers' CPNI as required by Section 64.2009 of the Commission's rules.

CBI takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the use of reasonable and proper authentication processes to identify a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or an in-store visit. CBI's policies prohibit a sales representative from disclosing call detail information over the phone, based on a customer-initiated telephone contact. Sales representatives are instructed to direct customers to obtain call detail via online account access or to mail the customer a duplicate bill to the street address of record. CBI has also implemented an authentication process for establishing online account access to call detail information without the use of readily available biographical information or account information. Finally, CBI policies require a customer to provide a photo ID to obtain access to CPNI/call detail information at CBI's retail store locations.

CBI has established a process for adding passwords to new and existing customer accounts without the use of readily available biographical information or account information. A customer who forgets an account password is required to present a photo ID at a retail store location to obtain access to CPNI, to make account changes, or to change a forgotten password.

CBI has also established a process for notifying customers of certain account changes as required by Section 64.2010(f) of the Commission's rules.

Notification of CPNI Security Breaches

CBI has policies and procedures in place to ensure compliance with Section 64.2011 of the Commission's rules. Sales representatives as well as network security personnel are directed to notify CBI's Security Office if they reasonably believe that a CPNI breach has occurred. CBI will notify law enforcement and its customers of the breach in accordance with the rule, and a record of the breach will be maintained for two years.